디지털산업정보학회 논문지 제12권 제1호-2016년 3월
http://dx.doi.org/10.17662/ksdim.2016.12.1.071

협력기반 인증 기법을 통한 라우팅 성능 개선에 관한 연구

양 환 석*

A Study on Routing Performance Improvement through Cooperation Authentication Technique

Yang Hwanseok

〈Abstract〉

The main security threats in MANET are integrity and non-repudiation. In the meantime, a lot of secure routing protocols have been designed in order to block these security threats. In this paper, partnership-based authentication technique is proposed in order to provide participation exclusion of network and non-repudiation for the nodes. The proposed technique is a technique that participates in data communication for only the nodes receiving the authentication through the authentication process for the nodes. For this, the proposed technique is largely consists of two steps. The first step is the process that issued the certificate after the reliability for the nodes participating in the network is evaluated. And in the second step, the key exchange agreement with the neighbor nodes is performed and data communication is made after setting security path with responding nodes. The level of security in data transmission is improved because the process of path setting is performed through cooperation with a neighboring nodes having high reliability during the course of these two steps. The superiority of proposed technique in this paper was confirmed through the comparative experiment.

Key Words : Cooperation Authentication, Trust Evaluation, Authentication Technique, MANET

Ⅰ. 서론

고정된 인프라 없이 무선 노드로만 구성된 MANET (Mobile Ad Hoc Network)은 전송 범위 내에 있는 노드들끼리 라우터 역할을 수행하면서 통신을 하는 네트워크이다[1]. 이러한 환경에 있는 이동 노드들은 정적인 노드들에 비해 제한된 자원과 낮은 처리능력 등의 특징을 가지고 있다. 또한 노드들의 이동으로 인해 발생하는 동적인 토폴로지는 경로 설정을 어렵게 하고 다양한 공격에 노출되어 있다. 이러한 많은 보안 문제를 해결하기 위해 그 동안 많은 연구가 진행되어 왔고, 그 중에서도 노드들에 대한 인증과 라우팅에 대해 많은 연구가 진행되어 왔다[2-3]. MANET에 존재하는 많은 공격들 중에서 라우팅 공격은 네트워크 전체 성능을 떨어뜨리기 때문에

*중부대학교 정보보호학과 조교수

매우 중요하다고 할 수 있다. 라우팅 공격은 도청과 같은 passive attack과 정상적인 패킷의 흐름을 방해하는 DoS와 같은 active attack이 있다[4]. 이러한 라우팅 공격을 사전에 차단하고 이동 노드들에게 이웃 노드들에 대한 신뢰성을 제공하여 목적 노드까지 안전한 경로를 설정할 수 있는 보안 라우팅을 제공해주는 것은 매우 중요하다고 할 수 있다[5].

본 논문에서는 안전한 경로 설정 및 데이터 통신을 보장하고 무결성과 부인방지를 위하여 협력기반 인증 기법을 제안하였다. 본 논문에서 제안한 협력기반 인증 기법은 크게 두 단계로 이루어져 있으며, 이를 위하여 계층 구조인 클러스터 형태를 이용하였다. 제안한 기법은 신뢰도 평가를 통해 인증서를 발급하는 첫 번째 단계와 보안 경로를 설정하는 두 번째 단계로 이루어져 있다. 노드들에 대한 신뢰 평가와 인증서 발급을 위하여 로컬 인증서버와 보조 인증 서버를 구성하였다. 로컬 인증 서버에서는 노드들에 대한 인증서 발급을 수행하는 역할을 담당하고 보조 인증 서버에서는 인증서 발급 요청 노드들에 대한 신뢰도 값을 평가 및 저장하고 있는 역할을 수행한다. 각 노드들에 대한 신뢰도 평가는 네트워크 참여한 노드들의 데이터 전송 값을 통해 이루어지며, 이 계산은 주기적으로 이루어지기 때문에 네트워크에 참여하면서 데이터 전송에 참여하지 않는 이기적인 노드들은 신뢰도 값이 낮아지게 된다. 이렇게 인증서를 발급받은 노드들은 안전한 경로 설정을 위해 자신의 공개키를 이웃 노드에 전송하여 이에 응답한 노드들과 보안 경로 설정 과정을 수행하게 된다. 이러한 과정을 통해 노드들에게 무결성과 부인방지를 제공해하고 라우팅 프로토콜의 보안 수준을 향상시키게 된다.

본 논문의 구성은 다음과 같다. 2장에서는 MANET의 인증 기법과 보안 라우팅 프로토콜에 대하여 살펴보고 3장에서는 본 논문에서 제안한 협력기반 인증 기법에 대하여 설명하였다. 4장에서는 실험을 통해 제안한 기법의 우수한 성능을 확인하였고 마지막으로 5장에서는 결론을 맺는다.

Ⅱ. 관련연구

2.1 MANET의 라우팅 프로토콜

MANET에서 사용되는 라우팅 프로토콜은 크게 노드의 위치정보를 사용하지 않는 프로토콜과 위치정보를 이용하는 프로토콜로 분류할 수 있다. 먼저, 노드들의 위치정보를 이용하지 않는 라우팅 프로토콜은 proactive와 reactive 방식으로 구분할 수 있다[6]. Proactive 라우팅 프로토콜은 노드들이 라우팅 정보를 주기적으로 교환하면서 전체 라우팅 정보를 유지하는 방식이다. 이 방식은 라우팅 정보를 지속적으로 유지하고 있기 때문에 목적 노드까지의 경로 발견 과정이 생략되어 패킷을 빠르게 전송할 수 있는 장점이 있다. 하지만 모든 노드가 주기적으로 라우팅 메시지를 방송하기 때문에 오버헤드가 크게 발생하는 단점을 가지고 있다[7]. Reactive 라우팅 프로토콜은 주기적으로 라우팅 메시지를 방송하는 것이 아니고 데이터 전송이 필요할 때만 목적 노드까지의 경로를 탐색하여 경로 정보를 얻는다. 따라서 경로 설정을 위한 오버헤드가 적은 장점을 가지고 있다. 하지만 패킷 전송시 경로 설정 시간이 길고 노드들의 이동으로 인한 경로 단절이 발생할 경우 경로 재탐색 과정을 거쳐야하기 때문에 패킷 전송 시간이 길어지는 단점이 있다[8]. 노드들의 위치정보를 이용하는 위치 기반 라우팅 프로토콜은 GPS를 이용하여 노드들의 위치 정보를 획득하여 이를 라우팅에 이용하는 방식이다. 이 방식은 목적 노드의 위치 정보와 beacon 메시지를 이용하여 경로 탐색을 확립을 한다. 이러한 특성 때문에 노드의 수와 상관없이 라우팅 오버헤드가 적은 장

점을 가지고 있다. 하지만 위치 정보만을 비교하여 패킷이 전달되기 때문에 잘못된 위치 정보에 의한 이웃 노드 선택은 더 이상 패킷을 전달할 수 없는 패킷 전달 오류가 빈번히 발생하는 단점이 있다[9].

2.2 보안 라우팅 기법

CBSR(Curve-Based Secure Routing) 기법은 CBGR에 암호화를 적용한 라우팅 기법으로서 크게 5단계의 과정으로 이루어져 있다[10].

1 단계 : 이웃 노드들에게 자신의 위치정보를 그룹키로 암호화하여 전송한다. 여기서 그룹키는 각 노드가 동일하게 가지고 있는 전역 키로서 사용된다.

2 단계 : 목적 노드에 자신의 위치와 필요한 정보를 키 체인중 하나로 암호화하여 전송한다.

3 단계 : 전역 키를 이용하여 암호화 키를 암호화한 후 방송 함

4 단계 : 소스 노드는 목적 노드로 커브를 생성하여 경로를 확립

5 단계 : 목적 노드는 수신한 패킷들의 내용을 비교하여 무결성을 확인

FBSR(Feedback based Secure Routing Protocol)은 평가함수를 이용하여 에너지 효율 지향적인 라우팅 프로토콜 기반으로써 MAC 계층의 인증인 단방향 해시 함수를 이용하여 보안을 제공하는 기법이다[11]. 이 기법은 이웃 노드로부터의 평가함수를 기초로 에너지 상태를 인지한다. 평가함수는 에너지 레벨과 거리의 조합을 이용하며 임계치 평가 함수에 의해 에너지 레벨이 이용된다. FBSR 기법에서는 라우팅 공격을 방지하기 위하여 두 가지 방법을 제공한다. 첫째로 이웃 노드로부터 오는 피드백은 단방향 해시 체인에 의해 서명되는 방법이고 두 번째는 공격 노드를 구분하기 위하여 베이스스테이션으로 오는 피드백을 활용하는 방법이다.

Ⅲ. 제안한 협력기반 보안인증 기법

본 장에서는 안전한 보안 경로 확립과 보안 데이터 전송을 제공하기 위하여 노드들간의 협력을 기반으로 한 인증 기법에 대하여 설명한다. 노드들에 대한 인증의 신뢰성을 향상시키기 위한 보조 인증 노드 기법을 적용하였다.

3.1 시스템 모델 및 구성 요소

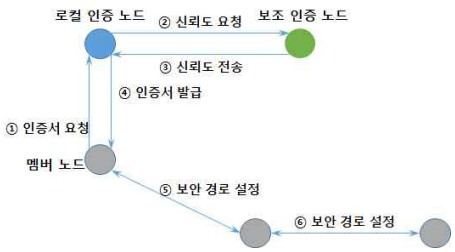
MANET에서 무결성 보장과 라우팅 메시지의 부인방지 기능을 제공하는 것은 네트워크 성능 유지 측면에서 중요하다. 특히 라우팅 공격으로 인한 피해는 다른 유형의 공격들에 비해 그 피해의 규모가 매우 크다. 따라서 본 논문에서는 노드들의 무결성과 부인 방지를 위하여 네트워크를 구성하는 노드들에 대한 신뢰도 검사를 통해 인증과정을 수행하고, 이 과정을 거친 노드들에 한해서 데이터 통신에 참여하도록 하였다. 이를 구현하기 위하여 계층형 네트워크 형태인 클러스터 구조를 이용하였으며, 이러한 형태는 중앙 관리, 즉 노드들에 대한 신뢰도를 검사하고 인증서 발급이 용이하다. 이러한 역할을 수행하는 노드를 로컬 인증 노드로 하였다. MANET을 구성하는 이동 노드들은 제한된 자원을 가지고 네트워크에 참여하기 때문에 한 노드에 많은 부하가 발생하면 해당 노드는 오랜 시간 제 역할을 수행할 수가 없게 된다. 따라서 노드들에 대한 정확한 신뢰 검사 및 인증을 위해 보조 인증 노드를 지정하였다. 본 논문에서 노드들의 협력기반 인증을 위한 각 노드들의 역할은 다음과 같다.

- 로컬 인증 노드 : 클러스터에 속한 모든 노드들

과 통신하면서 노드의 인증서 요청 발급에 대한 인증 관리를 수행하는 인증 서버 역할을 수행한다.

- 보조 인증 노드 : 클러스터내의 노드들에 대한 신뢰도 정보 확인 및 저장을 하는 노드로서 클러스터 내의 노드들이 데이터 전송에 참여한 정보를 수신하면 해당 정보를 확인한 후 신뢰도 값을 계산하는 역할을 수행한다.

네트워크 초기 구성 시 로컬 인증 노드 선택은 1-hop 거리에 가장 많은 이웃을 가지고 있는 노드, 즉 연결성이 가장 높은 노드를 선택하였으며, 보조 인증 노드는 두 번째로 높은 값을 가진 노드를 선택하였다. 네트워크에 참여하는 모든 노드들은 HELLO 메시지를 방송하여 자신의 1-hop 거리의 이웃 노드 존재를 알게 되고, 자신의 이웃 노드 수를 방송하여 로컬 인증 노드와 보조 인증 노드가 선출되게 된다. 이러한 과정을 통해 선출된 로컬 인증 노드와 보조 인증 노드는 클러스터 내의 노드들에게 자신의 존재를 알리게 된다. 클러스터 내의 노드들은 로컬 인증 노드에게 인증을 요청하고, 요청을 받은 인증 노드는 보조 인증 노드에게 해당 노드의 신뢰도 정보를 요청 및 수신한 후에 해당 노드에게 인증서를 발급받게 된다. 이렇게 인증서를 발급 받은 노드들에 한해서 데이터 전송에 참여할 수 있게 된다. <그림 1>은 노드들이 인증과정을 거쳐 데이터 통신에 참여하는 전체 과정을 보여주고 있다.



<그림 1> 제안한 협력인증 구조

3.2 협력기반 인증

노드들에 대한 안전하고 정확한 보안 인증 기법을 제공하기 위하여 협력기반 보안인증 기법을 제안하였다. 이를 위하여 보안인증 기법은 크게 2단계로 이루어져있다. 첫 번째 단계에서는 인증서 요청을 한 노드에 대한 신뢰도 검사가 이루어진다. 이때 해당 노드에 대한 신뢰도 검사는 보조 인증 노드의 협력을 통해 실행된다. 두 번째 단계는 보안 경로를 설정하는 단계로서 1-hop 거리의 이웃 노드들과 키 교환이 이루어지고 경로 발견과 경로 응답을 수행한다. 그리고 마지막으로 소스 노드와 목적 노드간의 데이터 전송이 이루어진다.

첫 번째 단계의 인증서 요청 과정은 다음과 같다. 먼저 네트워크에 참여하는 노드들은 자신이 속한 클러스터 내의 로컬 인증 노드에게 인증서를 요청한다. 인증서 발급 요청을 수신한 로컬 인증 노드는 보조 인증 노드에게 해당 노드의 신뢰도 정보를 요청하게 된다. 보조 인증 노드에서는 자신이 관리하는 신뢰 정보 테이블에 해당 노드의 신뢰도 값을 조회한 후 인증서 발급 여부를 통보하게 된다. 만약 자신의 신뢰 정보 테이블에 해당 노드의 정보가 존재하지 않는다면, 이웃 보조 인증 노드들에게 해당 노드의 신뢰 정보 요청을 방송하여 신뢰도 정보를 얻게 된다. 인증 노드로부터 발급받은 인증서에는 인증 ID, 발급시간, 만료시간 등의 정보가 포함되어 있다. 해당 노드는 인증서 만료기간 전에 반드시 인증서 갱신이 이루어져야 한다. 이는 노드들의 이기적인 행동을 방지하고 악의적인 노드들의 위장을 막기 위해 주기적인 신뢰도 평가를 수행해야하기 때문이다. <그림 2>는 위에서 설명한 인증서 발급 과정에 대한 pseudo code를 보여주고 있다.

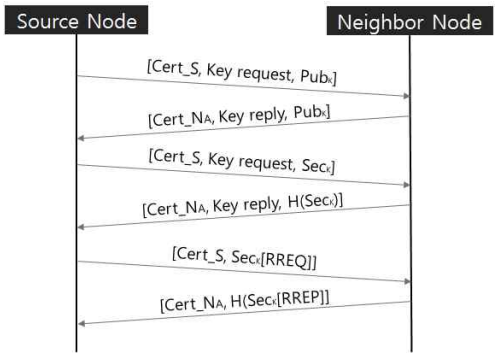
```
if(Request(Cert_ID))
{
    trust = SendtoSndCN(Node_ID);
    if(trust >= threshold)
    {
        issue(Node_ID(Cert));
        SendtoSndCN(Cert_info(Node_ID));
    }
    else
    {
        rejectMessage(Node_ID);
        SendtoSndCN(Black_List(Node_ID));
    }
}
```

<그림 2> 인증서 발급 pseudo code

두 번째 단계는 인증서를 발급받은 노드가 데이터 전송을 위해 안전한 보안 경로를 생성하는 과정이다. 이를 위해서 이웃 노드들과 키 교환 동의 단계가 실행된다. 즉, 데이터를 전송하고자하는 노드는 먼저 자신의 1-hop 거리의 이웃 노드들에게 자신의 공개키를 송신한다. 이를 수신한 이웃 노드들 중에서 송신 노드와 키 교환에 동의하는 노드들은 공개키와 자신의 해시로 서명된 공개키가 포함된 응답 메시지를 전송하게 된다. 이렇게 키 교환 동의에 응답한 이웃 노드들에게 송신 노드에서는 비밀키를 생성하고 이를 이웃 노드의 공개키로 암호화하여 전송하게 된다. 이를 수신한 이웃 노드는 송신 노드에게 응답하게 된다. 이렇게 응답을 한 이웃 노드들에게 목적 노드까지의 경로를 찾기 위한 RREQ 메시지를 전송하게 된다. 이러한 과정을 반복함으로써 이웃 노드와 안전하게 키 교환이 이루어진 노드들에게만 경로요청 메시지를 전송함으로써 목적 노드까지 보안 경로를 확립할 수 있게 된다. <그림 3>은 보안 경로 확립 과정을 보여주고 있다.

3.3 신뢰도 평가 및 관리

본 논문에서 제안한 노드들의 신뢰 평가는 네트워크에 참여하는 노드들에 대한 부인방지를 제공하고, 이기적인 행동을 막을 수 있는 기능을 제공하게 된다. 노드들에 대한 신뢰 평가는 보조 인증 노드에서

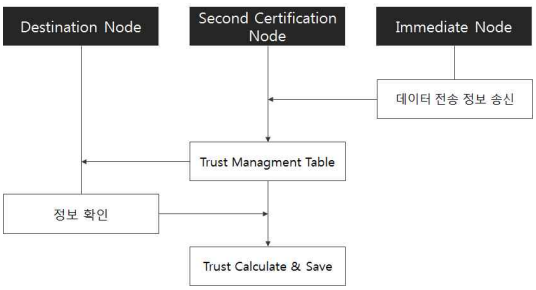


<그림 3> 보안 경로설정 과정

수집한 정보들에 의해 이루어진다. 보조 인증 노드에서 신뢰 정보의 수집 과정은 다음과 같다. 먼저 데이터 전송에 참여한 노드들은 자신이 데이터 전송에 참여한 정보를 보조 인증 노드에게 전달하게 된다. 이러한 데이터 전송 참여 정보를 수집한 보조 인증 노드는 데이터를 수신한 노드에게 해당 정보를 확인하는 과정을 거치게 된다. 이렇게 데이터 전송 정보에 대한 확인이 끝나면 해당 노드에 대한 신뢰도 값을 계산하여 지역 신뢰 테이블에 저장하게 된다. 신뢰도 계산은 식 (1)에 의해서 이루어진다.

$$T = \sum_{t=1}^{n} \frac{Acc(pkts) + Current(pkts)}{Rcv_t} \quad (1)$$

노드들의 신뢰도는 일정 시간동안에 데이터 전송에 참여하지 않으면 그 신뢰도는 점점 떨어지기 때문에 노드들의 이기적인 행동을 차단할 수 있게 된다. 그리고 노드들에 대한 평가된 신뢰값을 이용하여 인증서 발급 여부는 지역 신뢰 테이블에 저장된 전체 노드들의 신뢰도 값의 평균을 기준 값으로 하여 그 이상인 경우에만 인증서를 발급받을 수 있게 된다. <그림 4>는 위에서 설명한 신뢰 평가 정보 수집 및 계산 과정을 보여주고 있다.



<그림 4> 신뢰 정보수집 및 평가 과정

Ⅳ. 성능분석

4.1 실험 환경

본 논문에서 제안한 협력기반 인증 기법의 성능을 평가하기 위하여 ns-2 시뮬레이터를 이용하였으며, 20개의 악의적인 노드들을 구성하였다. 이들 중의 10개는 일정 시간동안 패킷을 포워딩 하지 않거나 폐기하고, 나머지는 라우팅 패킷 정보를 수정하는 공격을 실행하였다. 실험을 위해 사용한 환경변수 값은 <표 1>에서 보여주고 있다.

<표 1> 실험에 사용한 환경 변수

Parameter	Value
Network Size	1500 × 1500
Number of Nodes	100, 200
Pause Time(Sec)	20
Traffic Model	CBR
Packet Size	512

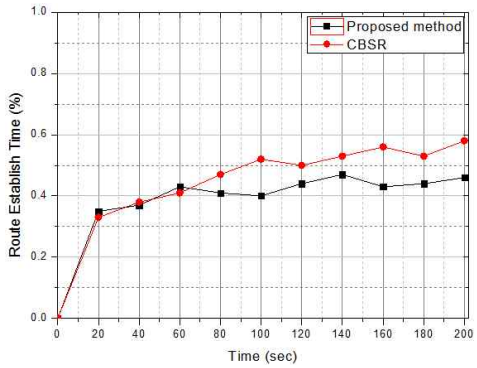
4.2 실험 결과

본 논문에서는 성능 평가를 위하여 제안한 협력기반 인증 기법과 유사한 클러스터 기반 보안 라우팅 기법을 적용한 CBSR 기법과 비교 실험하였다. 성능 측정의 평가 기준은 경로 설정 시간, 평균 지연시간, 처리율로 하였으며, 각각의 측정시 모든 실험 상황은 동일하게 설정하였다.

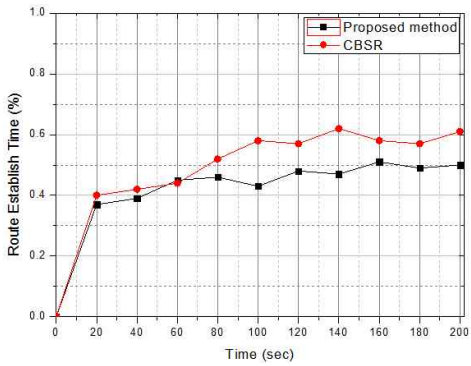
<그림 5>는 소스 노드와 목적 노드까지의 경로 설정 시간 결과를 보여주고 있다. CBSR 기법은 위치정보를 포함시킨 후 적절한 커브를 선택하고 이를 패킷에 인코딩을 시키고 중간 노드에서는 커브를 디코딩하여 다음 홉을 결정하는 방식을 통해 목적 노드까지의 경로를 동적으로 설정하기 때문에 경로 설정 시간이 길게 나타난다. 특히 악의적인 노드에 의해 패킷 전송이 지연되는 경우에 더욱 성능이 떨어지는 것을 확인할 수 있었다. 반면에 제안한 기법에서는 신뢰도가 낮은 노드들에 대한 참여를 배제시키기 때문에 경로 설정시 악의적인 노드에 크게 영향을 받지 않는 것을 실험 결과로 확인하였다.

<그림 6>에서 보여주고 있는 평균지연시간은 경로의 길이가 증가할수록 지연시간은 길어지게된다. CBSR 기법은 악의적인 노드들에 의해 경로발견 비율이 증가하기 때문에 평균지연시간 역시 길게 나타났다. 제안한 기법은 노드들에 대한 신뢰도 계산을 통한 인증과정을 거치기 때문에 악의적인 노드에 의한 경로발견 비율이 높지 않아 지연시간이 길지 않았다. 또한 악의적인 노드에 의한 경로정보 수정을 막기위해 노드들간의 키 교환 인증과정을 거치기 때문에 더욱 좋은 성능을 보여주었다. 다만 키 교환으로 인해 지연시간이 발생하였다.

<그림 7>에서는 처리율 실험 결과를 보여주고 있다. 그림에서처럼 악의적인 노드 수가 많아질수록 처리율이 낮아지는 것을 확인할 수 있다. CBSR 기법은 경로설정에 다중화를 이용하기 때문에 악의적인 노드 수에 비해 처리율이 많이 떨어지지는 않았으며, 제안한 기법은 네트워크에 참여하는 노드들의 이기적인 행동을 차단하고 키 교환 동의과정을 통해서 부인방지를 차단함으로써 처리율 성능이 우수함을 보

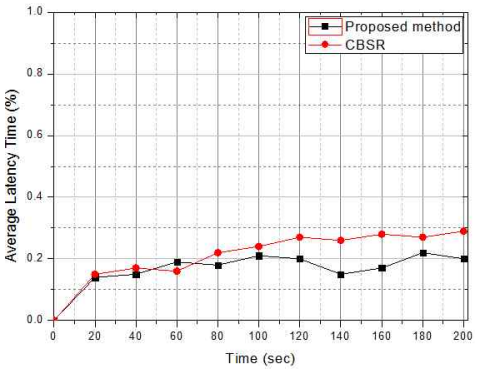


(a) 100 노드

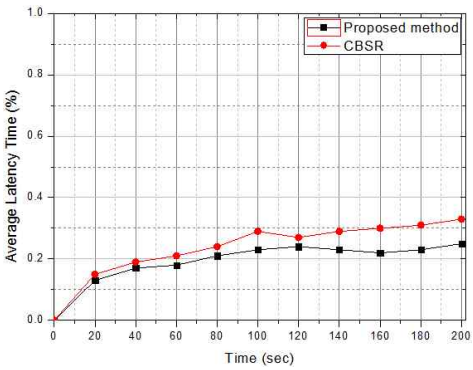


(b) 200 노드

<그림 5> 노드 수에 따른 경로 설정 시간



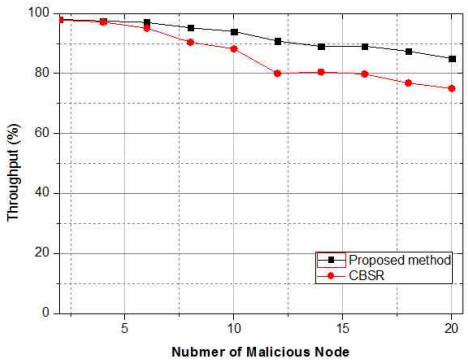
(a) 100 노드



(b) 200 노드

<그림 6> 노드 수에 따른 평균지연 시간

여주었다. 즉, 노드들에 대한 인증 성능이 우수함을 의미한다.



<그림 7> 처리율 측정 결과

Ⅴ. 결론

본 논문에서는 신뢰성 높은 라우팅 제공을 위하여 노드들의 간의 상호협력 인증 기법을 제안하였다. 이를 위하여 두단계의 과정으로 이루어져 있으며, 첫 번째 단계에서는 노드들에 대한 신뢰 평가를 통해 인증서를 발급하게 된다. 노드들의 인증서 발급을 위해 계층 구조인 클러스터 형태를 이용하였으며, 인증을

위해 로컬 인증 노드와 보조 인증 노드를 구성하였다. 보조 인증 노드는 클러스터내의 노드들이 네트워크에 참여한 정보를 확인 및 저장하는 역할을 수행하고, 로컬 인증 노드에서는 인증서 발급 역할을 담당한다. 보조 인증 노드에서는 데이터 전송 정보를 주기적으로 수집하여 노드들에 대한 신뢰도를 평가함으로써 노드들에 대한 이기적인 행동을 차단할 수 있게 하였다. 이렇게 인증서를 발급받은 노드들에 한해서 네트워크여 참여하도록 하였다. 두 번째 단계에서는 키 교환 동의를 통한 경로발견 단계이다. 데이터 전송을 위해 경로를 설정하기 위한 노드는 자신의 이웃 노드들에게 자신의 공개키를 전송하여 안전한 경로설정을 위해 참여할지 여부를 확인하는 키 교환 동의 과정을 수행하게 된다. 키 교환에 동의한 노드들을 통해서 목적 노드까지 안전한 경로를 설정하게 된다. 이와 같은 방법을 통해 경로설정이 수행함으로써 중간노드들에 의한 부인방지를 차단하였다. 본 논문에서 제안한 협력기반 인증 기법의 성능을 평가하기 위하여 CBSR 기법과 비교 실험하였으며, 경로 설정, 평균 지연, 처리율의 성능지표에서 평균 8. 3%의 우수한 성능을 보여주었다. 본 논문에서 제안한 기법은 이동 노드들의 전력 소모량을 고려하지 않았다. 향후 보안 라우팅을 위해 많아지는 트래픽을 양을 줄일 수 있는 기법과 전력 소모량에 대한 연구가 필요하다.

참고문헌

[1] J. Sen, “Robust and Efficient Node Authentication Protocol for Mobile Ad Hoc Networks,” Second International Conference on Computational Intelligence, Modelling and Simulation (CIMSiM), 2010, pp. 476-481.

[2] J. Sen, P. R. Chowdhury, I. Sengupta, “A distributed trust establishment scheme for mobile ad hoc networks,” in Proceedings of the International Conference on Computing: Theory and Applications, 2007, pp. 51-58.

[3] K. Naik (Joshi), A. Dixit, “Resource Aware Node Authentication Framework for Secure MANET,” IOSR Journal of Computer Engineering (IOSR-JCE), Vol. 16, 2014, pp. 109-113.

[4] 왕종수, 서두옥, “Sparse M2M 환경을 위한 DTMNs 라우팅 프로토콜,” 디지털산업정보학회지, 제10권, 제4호, 2014, pp. 11-18.

[5] M. K. Rafsanjani, A. Movaghar, “Identifying Monitoring Nodes with Selection of Authorized Nodes in Mobile Ad Hoc Networks,” World Applied Sciences Journal, Vol. 4, No. 3, 2008, pp. 444-449.

[6] Kush, A., Hwang, C., Gupta, P., “Secured Routing Scheme for Adhoc Networks,” International Journal of Computer Theory and Engineering (IJCTE) 3, Vol. 60, No. 1, 2013, pp. 1089-1098.

[7] P. Singh, M. Chandra Pandey, “Evaluation of certificate-based authentication in Mobile Ad-hoc networks,” International Conference on Recent Trends in Engineering and Technology, 2012.

[8] 왕종수, 서두옥, “극단적인 네트워크 환경을 위한 효율적인 라우팅 알고리즘,” 디지털산업정보학회지, 제8권, 제1호, 2012, pp. 47-53.

[9] Gomathi, S., Duraiswamy, K., “Guaranteed Packet Transfer in MANET”, In and Out of Coverage Areas and Energy Saving Using Random Casting (IJCSE) International Journal on Computer Science and Engineering 02(03),

2010, pp. 865-869.

[10] J. Sen, P. R. Chowdhury, and I. Sengupta, "A distributed trust establishment scheme for mobile ad hoc networks," in Proceedings of the International Conference on Computing: Theory and Applications, 2007, pp. 51-58.

[11] M. Cagalj, S. Capkun, and J. P. Hubaux, "Key Agreement in Peer-to-Peer Wireless Networks," Proceedings of IEEE, Special Issue on Security and Cryptography, Vol. 94, No. 2, 2006, pp. 467-478.

■ 저자소개 ■

양 환 석
Yang Hwanseok

2011년 9월~현재
중부대학교 정보보호학과 조교수
2006년 2월~2011년 2월
호원대학교 사이버수사경찰학과
연구교수
2005년 2월 조선대학교 전산통계학과
(이학박사)
1998년 2월 조선대학교 전산통계학과(이학석사)

관심분야 : 정보보호, 침입탐지시스템, MANET
E-mail : yanghs@joongbu.ac.kr

논문접수일: 2016년 2월 21일
수 정 일: 2016년 3월 9일
게재확정일: 2016년 3월 15일